MOODY'S
RATINGS

SECTOR IN-DEPTH
2 July 2024

✓ Send Your Feedback

Analyst Contacts

Cristiano Ventricelli *VP-Senior Analyst – DeFi & Digital Assets* cristiano.ventricelli@moodys.com	+39.02.91481.148
Rajeev Bamra *SVP-DeFi & Digital Assets Strategy* rajeev.bamra@moodys.com	+1.212.553.5878
Fabian Astic *Managing Director - Global Head of DeFi & Digital Asset* fabian.astic@moodys.com	+1.212.553.6814

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

Digital Economy — Bits, Bytes & Basis Points

Smart contract security standards are key to unlocking institutional adoption

Summary

Interview with Michael Lewellen and Steve Gant of OpenZeppelin, a smart contract security company. The views expressed by Michael Lewellen and Steve Gant in this report are their own views and not those of Moody's Ratings.

In our view, the capabilities of smart contracts have been a key driver in promoting the adoption of blockchain technology. Smart contracts are codes deployed on blockchains that enable them to execute programmable applications. They have the potential to reduce risks associated with third-party involvement, enhance efficiency, minimize costs, incorporate compliance rules and controls, and introduce transparency into digital agreements involving multiple parties. Although they do not yet serve as replacements for conventional legal agreements, the goal of smart contract developers is to render a variety of contract types both self-executing and self-enforcing. For the technology to gain wider acceptance, advancements in cybersecurity are key, and there is also a need for legal structures that guarantee the enforceability of smart contracts. We asked Michael Lewellen and Steve Gant from OpenZeppelin, which provides smart contract audit services, for their perspective on the future of the smart contract industry, including both opportunities and risks the technology and its users will face. Their responses are set out in question-and-answer format below and express OpenZeppelin's own perspectives on the topic, not those of Moody's Ratings.

Below is a summary of the key points from OpenZeppelin's responses to Moody's Ratings questions:

Standardizing smart contract practices across new frameworks becomes crucial. Numerous blockchain platforms are investigating alternative frameworks for smart contracts in search for improved scalability, privacy features and compatibility with a wider range of programming languages.

A balancing exercise between control and decentralization could improve smart contracts' regulatory compliance. Several decentralized finance (DeFi) protocols are employing a combination of measures that could mitigate adverse consequences that would occur if smart contracts were completely decentralized and immutable.

Smart contract security audits currently lack the uniform standards found in traditional finance. The growing importance of smart contracts will likely push security companies to unify their auditing procedures and create definitive guidelines that align with institutional needs.

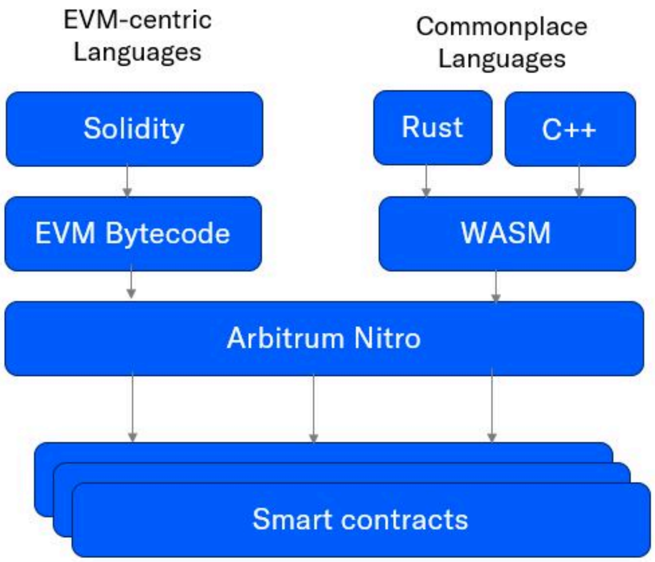
Q: As blockchain technology evolves, and particularly as blockchains emerge that are incompatible with the Ethereum Virtual Machine (EVM)[1], how will institutions maintain effective and standardized smart contract development and auditing practices across diverse blockchain formats?

At present, most blockchain platforms and smart contracts are built to support the Ethereum Virtual Machine (EVM,) for a variety of reasons: Ethereum and its programming language, Solidity, has the largest developer community, more mature tooling and libraries such as OpenZeppelin contracts[2], and more available security resources. While the EVM will likely remain significant in smart contract development for the foreseeable future, it does face scalability and usability challenges, especially in high-demand institutional settings.

Recognizing these limitations, many blockchain platforms are exploring alternative smart contract frameworks that offer enhanced scalability and privacy features, and support more widely used programming languages. Some networks, like Arbitrum with its Stylus framework, are even integrating these new options alongside traditional EVM-based contracts using WebAssembly (WASM), facilitating a gradual transition while maintaining some backward compatibility with EVM.

Exhibit 1

Example of a network providing new language support alongside Solidity



Source: OpenZeppelin

As the industry shifts from EVM-centric environments, standardizing smart contract practices across new frameworks becomes crucial. This involves identifying and unifying the key functionalities of EVM contracts so they perform consistently across different blockchains. For example, the USDC stablecoin operates on both EVM and non-EVM platforms by maintaining the core attributes of its original Ethereum-based ERC20 token.

Each new blockchain framework will require tailored security guidelines, informed by lessons learned from the EVM's challenges. Security auditing practices, however, should still follow universal security principles, such as preventing unauthorized access and avoiding logic errors. As blockchain technology diversifies, the goal is to ensure a smooth transition to these frameworks while upholding stringent security and functionality standards, enabling institutions to securely and effectively harness blockchain innovations.

This publication does not announce a credit rating action. For any credit ratings referenced in this publication, please see the issuer/deal page on https://ratings.moodys.com for the most updated credit rating action information and rating history.

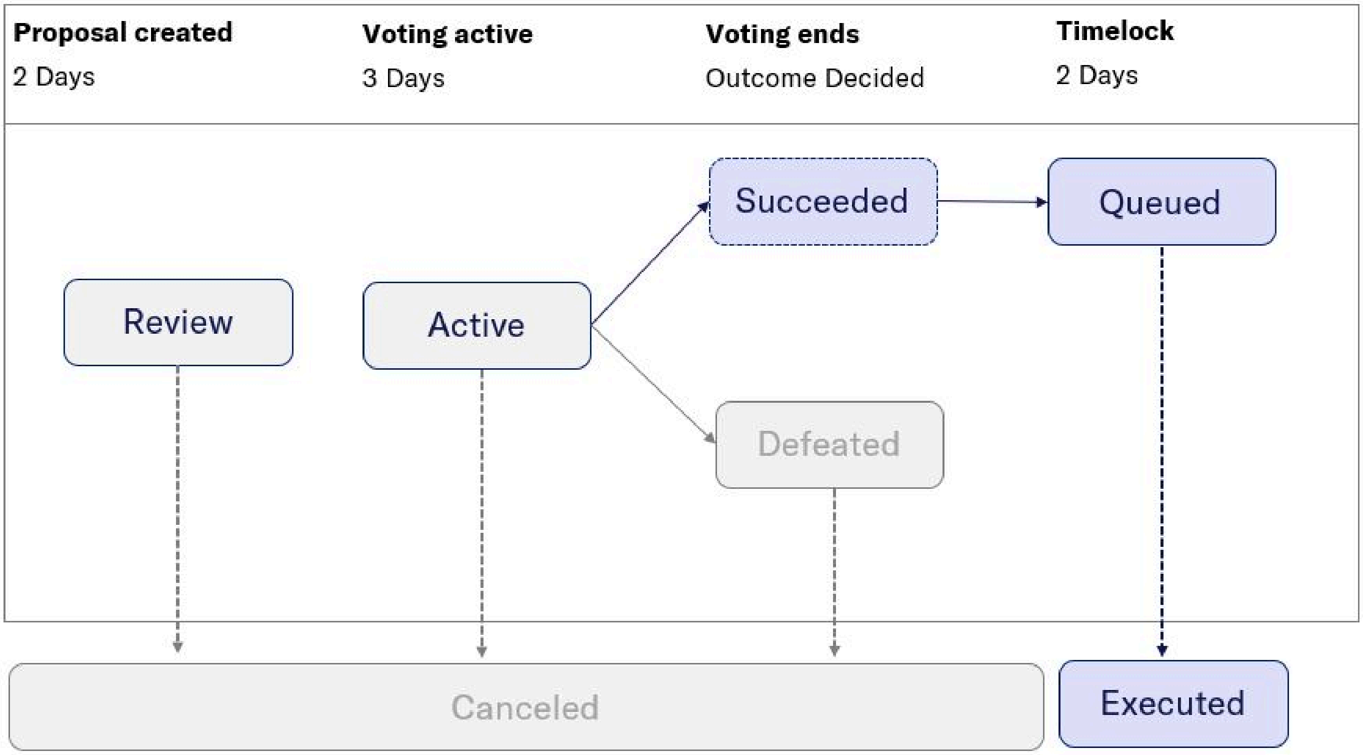
Q: Regulations are increasingly requiring the inclusion of 'kill switch' mechanisms in smart contracts, especially for institutional use cases, as a means to disable functions in an emergency – for example, in case of a cyberattack. How can developers integrate these features without compromising the contracts' decentralization and security?

The need for administrative controls has been in a long-running conflict with the decentralization ethos of the Web3 industry for many years. However, there are projects that are able to balance the need for emergency response actions while avoiding direct custodial access to funds.

For example, the Compound Finance lending protocol has a core set of smart contracts that currently manage billions of dollars in digital assets governed by a decentralized autonomous organization (DAO)[3], to manage risk factors and smart contract upgrades. They'll also contract security firms, such as OpenZeppelin, to perform audits on these upgrades and inform governance voters of the risks.

Exhibit 2

The process for passing a governance proposal on the Compound Finance DAO

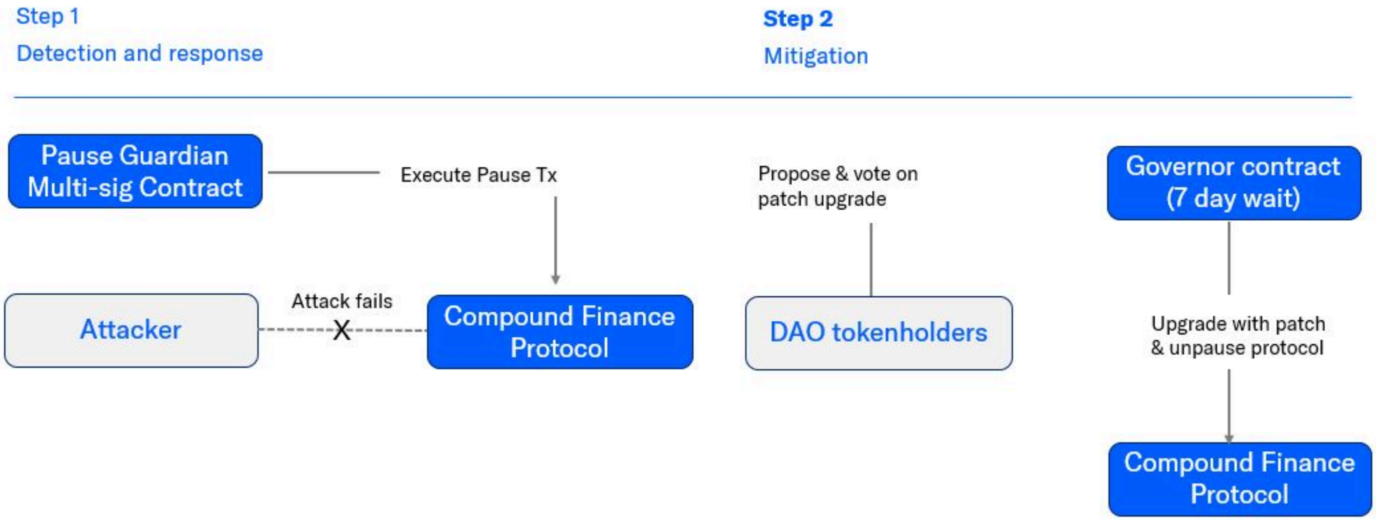


Source: OpenZeppelin

To address emergency situations such as a smart contract exploit, Compound Finance has a multi-signature (multi-sig)[4] council called the Pause Guardian that can pause select functionality in the protocol if a majority of the multi-sig signers agree. However, the Pause Guardian's powers are very limited and it cannot access user funds or change the smart contract's core logic. Only the DAO may later unpause the protocol and make changes to the smart contracts to patch an exploit, if any.

Exhibit 3

Example of Compound Finance DAO Security Council multi-sig pausing and governance response


Step 1
Detection and response
Step 2
Mitigation
Pause Guardian Multi-sig Contract
Execute Pause Tx
Attacker
Attack fails
Compound Finance Protocol
Propose & vote on patch upgrade
DAO tokenholders
Governor contract (7 day wait)
Upgrade with patch & unpause protocol
Compound Finance Protocol

Source: OpenZeppelin

With Compound Finance, we see one example where a "kill-switch" is available for emergency situations without giving custodial control of user funds to a third party. More substantial controls of smart contracts upgrades are protected with on-chain governance and "timelocks"[5] that give users time to remove their funds should they disagree with governance decisions.

Q: What innovative approaches are in use that strengthen access control in tokenized products – that is, solutions that keep firm guardrails around who can access, transfer or use tokens – particularly ones that meet the risk tolerance and compliance standards of institutional investors?

Several strategies are currently employed to enhance access control within tokenized environments. One common method is the use of on-chain blacklists, which prevent transactions involving listed addresses known for illicit activities or subject to legal restrictions, such as OFAC[6] sanctions. This approach is widely adopted by major stablecoins like Tether and USDC to maintain regulatory compliance and prevent misuse by unauthorized entities. A blacklist's effectiveness is often only limited by how quickly an operator can respond to live incidents, as some criminal activity may still occur before operators are able to freeze funds and blacklist bad actors that are identified.

Another prevalent method is the implementation of on-chain whitelists, which permit transactions only from addresses that have passed KYC checks and are approved by the token issuer. This method is particularly favored by institutional projects on public blockchains, allowing precise control over who can interact with their tokens. However, the adoption rate of such projects can be limited by the issuer's capacity to efficiently approve new participants, which can potentially restrict growth and integration within the broader digital finance ecosystem.

In addition to public blockchain solutions, some institutions opt for permissioned blockchain networks like Hyperledger Besu. These networks offer heightened control over network operations and are ideal for institutions testing blockchain solutions in a secure environment before potentially transitioning to a public blockchain. This staged approach helps institutions manage risks and compliance effectively while exploring broader blockchain applications.

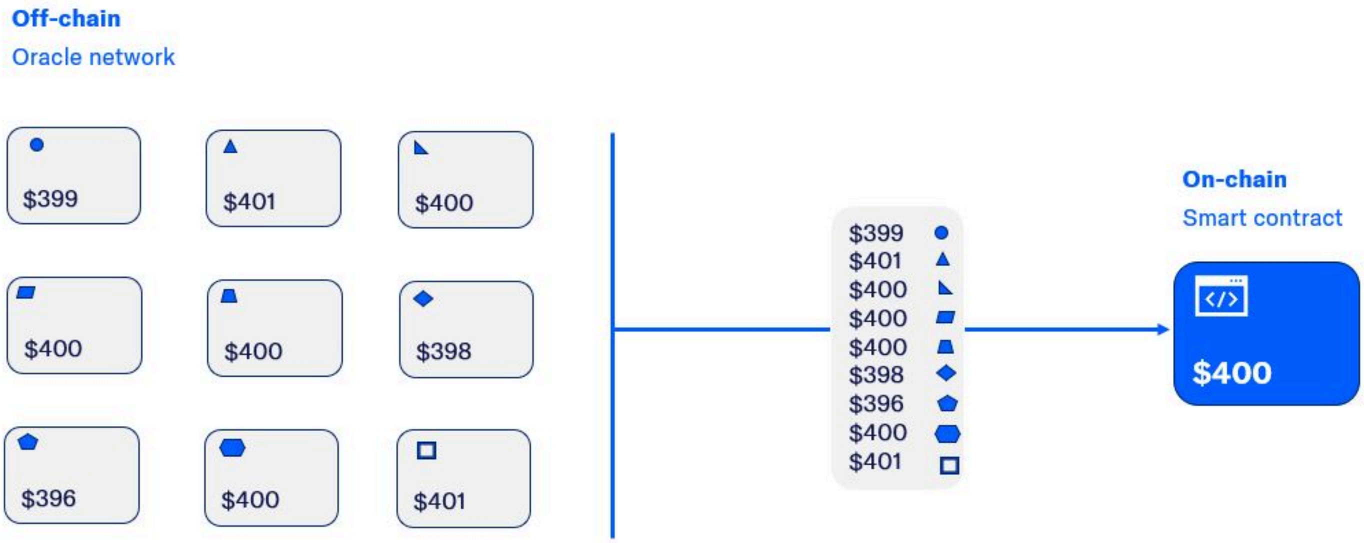
Overall, both blacklists and whitelists offer contrasting trade-offs in how they control access to tokenized products, balancing control with open access. Alternatively, using permissioned blockchains with access controlled at the network level is a viable solution to protect institutional token projects before they are ready to be deployed in a public environment.

Q: The integration of off-chain data through oracles is crucial for many smart contracts but introduces potential vulnerabilities, which could discourage institutional adoption. What ways are there to securely implement off-chain oracles within an institutional framework? How could these systems be structured to minimize the reliance on trust assumptions[7] and enhance the reliability of off-chain data feeds enough to meet institutional stakeholders' rigorous standards?

Oracles are essential for verifying off-chain events like market prices, ensuring smart contracts execute accurately. Leading oracle solutions, such as Chainlink, mitigate risks by aggregating data from multiple independent providers to provide a unified, averaged price feed. This redundancy reduces risks of inaccuracies, mimicking blockchain security, where integrity depends largely on honesty of the majority of blockchain network participants.

Exhibit 4

Example of an Oracle Network that aggregates multiple data providers to provide an average market price to a blockchain smart contract



Source: OpenZeppelin

Operators are selected for their reliability and trustworthiness, minimizing data interruption risks. Institutions should also prepare for emergencies by having fallback oracles ready.

On-chain price oracles from decentralized exchanges can be used, but require careful risk assessment because of potential liquidity issues and susceptibility to manipulation. This approach helps ensure data reliability for institutional-grade smart contracts.

Additionally, institutions can consider on-chain price oracles sourced from decentralized exchanges and other blockchain-based markets, which can be used to calculate prices based on a time-weighted average price (TWAP). However, as a result of typically lower liquidity and greater susceptibility to manipulation in these markets, such on-chain oracles should be used cautiously and supplemented with thorough risk assessment strategies.

Q: As smart contract interactions increase in complexity, explaining them clearly to all stakeholders becomes more difficult, particularly for institutional stakeholders seeking transparency and risk mitigation. How can institutions describe smart contracts in a way that is useful to developers, auditors, and end-users? Are there any initiatives to standardize smart contract documentation or visualization?

Smart contract interaction can indeed become very complex. The combination of many different smart contract protocols in a single transaction or trading strategy can make it incredibly difficult to parse what is going on and what risks are being incurred.

One ongoing effort to improve transparency is the standardization of smart contract primitives[8]. ERCs[9] are a long-running community effort to standardize common features such as fungible tokens (ERC-20), NFTs[10](ERC-721) and tokenized vaults (ERC-4626). Through these standards, interoperability is made easier with many wallets and visualization tools able to more easily parse transfers and support newly created assets without custom integrations.

With better native support for traceability and further standardization of common primitives, we expect that visualization tools such as Etherscan will become more streamlined and accessible to both common users and financial institutions to better understand smart contract interactions.

Q: How do you perceive the differences between the smart contract audit processes for digital finance projects and those in traditional finance? Are there specific considerations, risk assessments, or compliance checks that are required in institutional audits only? How would you suggest auditors tailor their approaches to address the regulatory and security needs of institutional clients?

Currently, smart contract security audits lack uniform standards like those found in traditional finance, such as SOC 2[11]. Each blockchain security firm must continuously update its knowledge of the latest exploits and best practices to effectively evaluate smart contracts. This variation can challenge clients trying to gauge the quality of security services without deep industry knowledge.

A key difference in security approaches lies in the nature of the data: traditional finance focuses on protecting private customer data, whereas blockchain data is typically public. Therefore, smart contract audits concentrate more on securing digital assets from theft and ensuring the enforcement of their foundational rules within an open, permissionless ecosystem. This task is complicated by the fact that blockchain systems are inherently open, with publicly accessible source code and network structures, making them potentially vulnerable to external attacks.

As smart contracts become more prevalent, there is an increasing need for security firms to standardize their audit processes and establish clear guidelines that meet institutional requirements. Initiatives like EEA EthTrust are working toward standardizing smart contract audits, though widespread adoption is slow due to the industry's rapid evolution and decentralized nature. Nevertheless, these emerging standards are crucial for providing a framework to assess smart contract risks accurately.

Moreover, other aspects of blockchain systems — such as cryptographic keys, network endpoints, and associated web applications — still benefit from adhering to traditional security standards, ensuring a comprehensive approach to institutional blockchain security. As smart contract use expands, institutions will likely want to assess security at every level of the blockchain stack to create a cohesive threat model and security assessment.

Endnotes

[1] The Ethereum Virtual Machine (EVM) is a decentralized virtual environment that executes code consistently and securely across all Ethereum nodes.

[2] See https://www.openzeppelin.com/contracts

[3] A DAO is an organization without central leadership. It is governed by a community organized by rules encoded on a public blockchain.

[4] Multi-sig, also called multi-signature, is the requirement for a transaction to have two or more signatures before it can be executed.

[5] Timelock smart contracts, also known as time-based or delayed contracts, are a specialized type of smart contract that introduces a delay or time-based constraint on the execution of certain actions or transactions.

[6] The Office of Foreign Assets Control (OFAC) is a financial intelligence and enforcement agency of the US Treasury Department. It administers and enforces economic and trade sanctions in support of US national security and foreign policy objectives.

[7] Trust assumptions pertain to the belief that various parts of a system, such as off-chain data sources or oracles, are providing accurate and trustworthy information.

[8] Smart contract primitives are foundational functions that serve as the building blocks for creating more complex logic and applications.

[9] An Ethereum Request for Comment (ERC) is a formal proposal or standardization document that outlines a specific improvement or extension for the Ethereum blockchain.

[10] A non-fungible token (NFT) is a non-interchangeable digital asset. NFTs typically reference digital files such as photos, videos, and audio.

[11] SOC 2, also known as Service Organization Control Type 2, is a cybersecurity compliance framework developed by the American Institute of Certified Public Accountants (AICPA). The primary purpose of SOC 2 is to ensure that third-party service providers store and process client data in a secure manner.

CREDIT RATINGS ISSUED BY MOODY'S CREDIT RATINGS AFFILIATES ARE THEIR CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES, AND MATERIALS, PRODUCTS, SERVICES AND INFORMATION PUBLISHED OR OTHERWISE MADE AVAILABLE BY MOODY'S (COLLECTIVELY, "MATERIALS") MAY INCLUDE SUCH CURRENT OPINIONS. MOODY'S DEFINES CREDIT RISK AS THE RISK THAT AN ENTITY MAY NOT MEET ITS CONTRACTUAL FINANCIAL OBLIGATIONS AS THEY COME DUE AND ANY ESTIMATED FINANCIAL LOSS IN THE EVENT OF DEFAULT OR IMPAIRMENT. SEE APPLICABLE MOODY'S RATING SYMBOLS AND DEFINITIONS PUBLICATION FOR INFORMATION ON THE TYPES OF CONTRACTUAL FINANCIAL OBLIGATIONS ADDRESSED BY MOODY'S CREDIT RATINGS. CREDIT RATINGS DO NOT ADDRESS ANY OTHER RISK, INCLUDING BUT NOT LIMITED TO: LIQUIDITY RISK, MARKET VALUE RISK, OR PRICE VOLATILITY. CREDIT RATINGS, NON-CREDIT ASSESSMENTS ("ASSESSMENTS"), AND OTHER OPINIONS INCLUDED IN MOODY'S MATERIALS ARE NOT STATEMENTS OF CURRENT OR HISTORICAL FACT. MOODY'S MATERIALS MAY ALSO INCLUDE QUANTITATIVE MODEL-BASED ESTIMATES OF CREDIT RISK AND RELATED OPINIONS OR COMMENTARY PUBLISHED BY MOODY'S ANALYTICS, INC. AND/OR ITS AFFILIATES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS DO NOT CONSTITUTE OR PROVIDE INVESTMENT OR FINANCIAL ADVICE, AND MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS DO NOT COMMENT ON THE SUITABILITY OF AN INVESTMENT FOR ANY PARTICULAR INVESTOR. MOODY'S ISSUES ITS CREDIT RATINGS, ASSESSMENTS AND OTHER OPINIONS AND PUBLISHES OR OTHERWISE MAKES AVAILABLE ITS MATERIALS WITH THE EXPECTATION AND UNDERSTANDING THAT EACH INVESTOR WILL, WITH DUE CARE, MAKE ITS OWN STUDY AND EVALUATION OF EACH SECURITY THAT IS UNDER CONSIDERATION FOR PURCHASE, HOLDING, OR SALE.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS, AND MATERIALS ARE NOT INTENDED FOR USE BY RETAIL INVESTORS AND IT WOULD BE RECKLESS AND INAPPROPRIATE FOR RETAIL INVESTORS TO USE MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS OR MATERIALS WHEN MAKING AN INVESTMENT DECISION. IF IN DOUBT YOU SHOULD CONTACT YOUR FINANCIAL OR OTHER PROFESSIONAL ADVISER.

ALL INFORMATION CONTAINED HEREIN IS PROTECTED BY LAW, INCLUDING BUT NOT LIMITED TO, COPYRIGHT LAW, AND NONE OF SUCH INFORMATION MAY BE COPIED OR OTHERWISE REPRODUCED, REPACKAGED, FURTHER TRANSMITTED, TRANSFERRED, DISSEMINATED, REDISTRIBUTED OR RESOLD, OR STORED FOR SUBSEQUENT USE FOR ANY SUCH PURPOSE, IN WHOLE OR IN PART, IN ANY FORM OR MANNER OR BY ANY MEANS WHATSOEVER, BY ANY PERSON WITHOUT MOODY'S PRIOR WRITTEN CONSENT. FOR CLARITY, NO INFORMATION CONTAINED HEREIN MAY BE USED TO DEVELOP, IMPROVE, TRAIN OR RETRAIN ANY SOFTWARE PROGRAM OR DATABASE, INCLUDING, BUT NOT LIMITED TO, FOR ANY ARTIFICIAL INTELLIGENCE, MACHINE LEARNING OR NATURAL LANGUAGE PROCESSING SOFTWARE, ALGORITHM, METHODOLOGY AND/OR MODEL.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS ARE NOT INTENDED FOR USE BY ANY PERSON AS A BENCHMARK AS THAT TERM IS DEFINED FOR REGULATORY PURPOSES AND MUST NOT BE USED IN ANY WAY THAT COULD RESULT IN THEM BEING CONSIDERED A BENCHMARK.

All information contained herein is obtained by MOODY'S from sources believed by it to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, all information contained herein is provided "AS IS" without warranty of any kind. MOODY'S adopts all necessary measures so that the information it uses in assigning a credit rating is of sufficient quality and from sources MOODY'S considers to be reliable including, when appropriate, independent third-party sources. However, MOODY'S is not an auditor and cannot in every instance independently verify or validate information received in the credit rating process or in preparing its Materials.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability to any person or entity for any indirect, special, consequential, or incidental losses or damages whatsoever arising from or in connection with the information contained herein or the use of or inability to use any such information, even if MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers is advised in advance of the possibility of such losses or damages, including but not limited to: (a) any loss of present or prospective profits or (b) any loss or damage arising where the relevant financial instrument is not the subject of a particular credit rating assigned by MOODY'S.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability for any direct or compensatory losses or damages caused to any person or entity, including but not limited to by any negligence (but excluding fraud, willful misconduct or any other type of liability that, for the avoidance of doubt, by law cannot be excluded) on the part of, or any contingency within or beyond the control of, MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers, arising from or in connection with the information contained herein or the use of or inability to use any such information.

NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY CREDIT RATING, ASSESSMENT, OTHER OPINION OR INFORMATION IS GIVEN OR MADE BY MOODY'S IN ANY FORM OR MANNER WHATSOEVER.

Moody's Investors Service, Inc., a wholly-owned credit rating agency subsidiary of Moody's Corporation ("MCO"), hereby discloses that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by Moody's Investors Service, Inc. have, prior to assignment of any credit rating, agreed to pay to Moody's Investors Service, Inc. for credit ratings opinions and services rendered by it. MCO and Moody's Investors Service also maintain policies and procedures to address the independence of Moody's Investors Service credit ratings and credit rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold credit ratings from Moody's Investors Service, Inc. and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at www.moodys.com under the heading "Investor Relations — Corporate Governance — Charter Documents - Director and Shareholder Affiliation Policy."

Moody's SF Japan K.K., Moody's Local AR Agente de Calificación de Riesgo S.A., Moody's Local BR Agência de Classificação de Risco LTDA, Moody's Local MX S.A. de C.V, I.C.V., Moody's Local PE Clasificadora de Riesgo S.A., and Moody's Local PA Calificadora de Riesgo S.A. (collectively, the "Moody's Non-NRSRO CRAs") are all indirectly wholly-owned credit rating agency subsidiaries of MCO. None of the Moody's Non-NRSRO CRAs is a Nationally Recognized Statistical Rating Organization.

Additional terms for Australia only: Any publication into Australia of this document is pursuant to the Australian Financial Services License of MOODY'S affiliate, Moody's Investors Service Pty Limited ABN 61 003 399 657AFSL 336969 and/or Moody's Analytics Australia Pty Ltd ABN 94 105 136 972 AFSL 383569 (as applicable). This document is intended to be provided only to "wholesale clients" within the meaning of section 761G of the Corporations Act 2001. By continuing to access this document from within Australia, you represent to MOODY'S that you are, or are accessing the document as a representative of, a "wholesale client" and that neither you nor the entity you represent will directly or indirectly disseminate this document or its contents to "retail clients" within the meaning of section 761G of the Corporations Act 2001. MOODY'S credit rating is an opinion as to the creditworthiness of a debt obligation of the issuer, not on the equity securities of the issuer or any form of security that is available to retail investors.

Additional terms for India only: Moody's credit ratings, Assessments, other opinions and Materials are not intended to be and shall not be relied upon or used by any users located in India in relation to securities listed or proposed to be listed on Indian stock exchanges.

Additional terms with respect to Second Party Opinions (as defined in Moody's Investors Service Rating Symbols and Definitions): Please note that a Second Party Opinion ("SPO") is not a "credit rating". The issuance of SPOs is not a regulated activity in many jurisdictions, including Singapore. JAPAN: In Japan, development and provision of SPOs fall under the category of "Ancillary Businesses", not "Credit Rating Business", and are not subject to the regulations applicable to "Credit Rating Business" under the Financial Instruments and Exchange Act of Japan and its relevant regulation. PRC: Any SPO: (1) does not constitute a PRC Green Bond Assessment as defined under any relevant PRC laws or regulations; (2) cannot be included in any registration statement, offering circular, prospectus or any other documents submitted to the PRC regulatory authorities or otherwise used to satisfy any PRC regulatory disclosure requirement; and (3) cannot be used within the PRC for any regulatory purpose or for any other purpose which is not permitted under relevant PRC laws or regulations. For the purposes of this disclaimer, "PRC" refers to the mainland of the People's Republic of China, excluding Hong Kong, Macau and Taiwan.

REPORT NUMBER 1398361

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454